UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/758,852	01/16/2004	Frank J. Hammond II	413127	6951

30955 7590 04/28/2009

LATHROP & GAGE LLP
4845 PEARL EAST CIRCLE
SUITE 201
BOULDER, CO 80301

EXAMINER	
TRAN, ELLEN C	
ART UNIT	PAPER NUMBER
2433	

MAIL DATE	DELIVERY MODE
04/28/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/758,852	HAMMOND ET AL.	
	Examiner	Art Unit	
	ELLEN TRAN	2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 February 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2 and 4-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, and 4-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Detailed Action

1. This action is responsive to communication filed on: 10 February 2009 with acknowledgement of an original application filed on 16 January 2004 with the benefit of a provisional application filed 16 January 2003.

2. Claims 1, 2, and 4-19, are pending; Claims 1, 14, 15, and 18 are independent claims; claim 1 and 18 have been amended. Claim 3 has been canceled. Amendments to the claims are accepted.

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10 February 2009 has been entered.

Response to Arguments

4. Applicant's arguments filed 10 February 2009 have been fully considered however they are moot due to new grounds of rejection below.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1, and 3-9,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Njemanze et al. U.S. Patent No. 7,219,239 (hereinafter '239) in view of Ghanea-Hercock U.S. Patent No. 7,370,358 (hereinafter '358) in further view of Yadav U.S. Patent Application Publication 2004/0123141 (hereinafter '141).

As to independent claim 1, "A method of protecting an electronic network, comprising: installing two or more agents within components of the electronic network; logically connecting the agents into one or more cooperative agent cells, each agent communicating with at least one other agent within the cooperative agent cell" is taught in '239 col. 5, lines 12-37;

the following is not explicitly taught in '239:

"performing an initial assessment of the electronic network to determine normal activity, using one or more of the agents" however '358 teaches determining normal behavior in col. 3, lines 6-26;

"monitoring the electronic network for abnormal activity using the agents" however '358 teaches monitoring the activity in col. 12, lines 32-40;

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system of a cooperative response to threat to domain security taught in '239 to include a mechanism to perform an initial assessment. One of ordinary skill in the art would have been motivated to perform such a modification to improve the efficiency of protection required by the increasingly sophisticated attacks see '358 (col. 1, lines 19 et seq.)

the following is not explicitly taught in '239 and '338:

"and protecting the electronic network by blocking the abnormal activity using the agents" however '141 teaches the agents block the abnormal activity by shutting down an application in paragraph 52.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system of a cooperative response to threat to domain security taught in '239 and '358 to include a mechanism to stop an attack. One of ordinary skill in the art would have been motivated to perform such a modification because of the many inadequacies in current detection systems see '141 (paragraph 5).

As to dependent claim 2, "wherein the step of installing comprises the step of installing a type 2 super peer agent for authenticating, authorizing and reauthorizing the agents" is taught in '239 col. 20, lines 26-55.

As to dependent claim 4, "wherein the step of installing further comprises: establishing bidirectional communication protocols for agent communication within the cooperative agent cells; delegating one or more agents in the cooperative agent cells to have bidirectional communication with another delegated agent; and establishing bidirectional communication protocols for each delegated agent to communicate with another delegated agent" is shown in '239 col. 3, lines 4-10 and col. 22, lines 27-31.

As to dependent claim 5, "wherein the step of installing further comprises: broadcasting a request for agents to submit to authentication; and authenticating submitted agents" is disclosed in '239 col. 21, lines 1-40.

As to dependent claim 6, "wherein the step of logically connecting further comprises self-organizing at least one of the agents into each of the cooperative agent cells" is taught in '239 col. 13, lines 13-31 and col. 7, lines 6-20.

As to dependent claim 7, "wherein the step of establishing further comprising communicating via at least one covert communication protocol" is shown in '239 col. 8, lines 18-60.

As to dependent claim 8, "wherein the step of performing an initial assessment comprises: mapping systems, communication ports and attached devices of the electronic network; and establishing normal activity of the systems, communication ports, and attached devices" is disclosed in '239 col. 6, lines 51-67.

As to dependent claim 9, "wherein the step of monitoring comprises: non-destructively intercepting communications on the electronic network; collecting events from the intercepted communications; and determining if the events indicate abnormal activity" is taught in '358 col. 3, lines 32-40.

7. **Claims 15-19,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Njemanze et al. U.S. Patent No. 7,219,239 (hereinafter '239) in view of Ghanea-Hercock U.S. Patent No. 7,370,358 (hereinafter '358).

As to independent claim 15, "A system for monitoring events within an electronic network, comprising: a cooperative agent network having two or more agents, each agent installed within one component of the electronic network, the two or more agents forming at least one cooperative cell for collecting events from the electronic network, the cooperative agent network further comprising:" is taught in '239 col. 5, lines 12-37;

"one or more event correlation engines, each event correlation engine being connected to the electronic network and having a receive event handler for receiving the events addressed to the event correlation engine" is shown in '239 col. 2, lines 16-28; the following is not explicitly taught in '239:

"and one or more event correlation modules, each of the event correlation modules having an event pattern that defines events of interest" however '358 teaches determining patterns of interest in col. 2, lines 32-40;

"each of the correlation modules receiving all events received by the event correlation engine, the event correlation module correlating the events of interest" however 358 teaches the nominated agent can compare the recorded patterns to protect the network in col. 4, line 54 through col. 5, line 13.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system of a cooperative response to threat to domain security taught in '239 to include a mechanism to perform an initial assessment. One of ordinary skill in the art would have been motivated to perform such a modification to improve the efficiency of protection required by the increasingly sophisticated attacks see '358 (col. 1, lines 19 et seq.)

As to dependent claim 16, "wherein the event correlation module is a simulated annealing correlator module" is taught in '358 col. 4, line 54 through col. 5, line 13.

As to dependent claim 17, "the simulated annealing correlator further comprising: recorded events; a simulated annealing correlator engine; heuristics; and a correlation threshold; wherein the simulated annealing correlator engine utilizes the heuristics and the correlation threshold to correlate the events received by the event correlation engine with

the recorded events, the correlated events being added to the recorded events" is shown in '358 col. 4, line 54 through col. 5, line 13.

As to independent claim 18, "collecting electronic network events; sampling the electronic network events with one or more event correlation engines" is shown in '239 col. 2, lines 16-28;

the following is not explicitly taught in '239:

"A method of pattern recognition, comprising: performing an initial assessment of the electronic network" " however '358 teaches determining normal behavior in col. 3, lines 6-26;

"passing sampled electronic network events from each event correlation engine to one or more event correlator modules within each event correlation engine; comparing events in each of the event correlator modules by sampling the events, determining if any of the events matches an event pattern, and, if there is a match, creating a new event announcing the match and passing the new event to the associated event correlation engine for electronic network distribution and determining patterns in events using a simulated annealing correlator, determining if the pattern is important, and, if so, creating a new event announcing the important pattern and passing the new event to the associated event correlation engine for network distribution" however 358 teaches the nominated agent can compare the recorded patterns to protect the network in col. 4, line 54 through col. 5, line 13.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system of a cooperative response to threat to domain security taught in '239 to include a mechanism to perform an initial assessment. One of ordinary skill in the art would

have been motivated to perform such a modification to improve the efficiency of protection required by the increasingly sophisticated attacks see '358 (col. 1, lines 19 et seq.)

As to dependent claim 19, "wherein the step of sampling further comprises sampling all of, or less than all of, the electronic network events" is taught in '358 col. 4, line 54 through col. 5, line 13.

8. **Claims 10 and 14,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Njemanze et al. U.S. Patent No. 7,219,239 (hereinafter '239) in view of Ghanea-Hercock U.S. Patent No. 7,370,358 (hereinafter '358) in further view of Yadav U.S. Patent Application Publication 2004/0123141 (hereinafter '141) in further view of Moran U.S. Patent No. 7,085,936 (hereinafter '936).

As to dependent claim 10, the following is not explicitly taught in the combination of teaching of '239, '358, and '141: **"wherein the step of protecting comprises one or more of: luring a malicious agent that causes abnormal activity into a false appearance of success; planting instructions on information retrieved by the malicious agent to assist in identifying the origins of the malicious agent"** however '936 teaches that the system includes a trap system create a virtual cage in col. 7, lines 42-51;

"isolating electronic network components which have been compromised by the malicious agent; attacking the malicious agent; formulating a strategy to eliminate recently discovered vulnerabilities in the electronic network; installing patches to eliminate vulnerabilities in the electronic network; reassessing the electronic network to detect

abnormal operations; and investigating abnormal operations of the electronic network" however '936 teaches "The inventive system focuses on discovering and presenting information about an attack, and presents configuration problems that are likely related to the attack, while suppressing those that aren't. Additionally, the presentation may show where relevant configuration problems fit within the factors that made the attack possible. This facilitates recovering from the attack, because the system administrator may be able to block future attacks of the same type by fixing only a subset of factors involved rather than having to fix every possible factor. It is also extremely useful in situations where one of the configuration problems cannot be changed due to its providing crucial functionality for the enterprise. For example, the restore command should normally not be set to allow execution by normal users with SetUID to root because it can be used to allow a normal user to install his own SetUID program on the computer that gives him a root shell. However, the dump-restore command pair have features that make them preferable in various circumstances to the other commonly available archiving and file copying utilities, and thus a system administrator may decide that having this capability available is worth the security risk" in col. 12, lines 9-29.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system of a cooperative response to threat to domain security taught in '239, 338, and '141 to include a mechanism to quarantine attacked systems. One of ordinary skill in the art would have been motivated to perform such a modification because of the need to improve existing intrusion detection systems see '936 (col. 3, lines 3 et seq.)

9. **Claims 11-13,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Njemanze et al. U.S. Patent No. 7,219,239 (hereinafter '239) in view of Ghanea-Hercock U.S. Patent No. 7,370,358 (hereinafter '358) in further view of Yadav U.S. Patent Application Publication 2004/0123141 (hereinafter '141) in further view of Rowland et al. U.S. Patent No. 7,058,968 (hereinafter '968).

As to dependent claim 11, the following is not explicitly taught in the combination of teaching of '338 and '499: **"further comprising promoting one of the agents in each of the cooperative agent cells to a cell delegate"** however '968 teaches that the architecture of the system is designed to allow modularity. This modularity allows for the roles to be reversed. In col. 4, lines 44-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system of a cooperative response to threat to domain security taught in '239, 338, and '141 to include a means to develop a hierarchical agent installation promoting agents. One of ordinary skill in the art would have been motivated to perform such a modification because of the need to allow for flexibility for mobile autonomous agents see '968 (col. 1, lines 58 et seq.).

As to dependent claim 12, "further comprising: promoting a second agent in each of the cooperative agent cells to a type 1 super peer agent; authenticating new agents with the type 1 super peer agent; and communicating between the cooperative agent cells and a command and control console via the cell delegate to protect the network from malicious activity" however '968 teaches that the architecture of the system is designed to allow modularity. This modularity allows for the roles to be reversed. In col. 4, lines 44-67.

As to dependent claim 13, "the agents and cooperative agent cells being configured for independent and collaborative investigation of the electronic network, isolation of compromised components of the electronic network, and defense of the electronic network" however '968 teaches that the architecture of the system is designed to allow modularity. This modularity allows for the roles to be reversed. In col. 4, lines 44-67.

12. **Claim 14,** is rejected under 35 U.S.C. 103(a) as being unpatentable over Njemanze et al. U.S. Patent No. 7,219,239 (hereinafter '239) in view of Ghanea-Hercock U.S. Patent No. 7,370,358 (hereinafter '358) in further view of Yadav U.S. Patent Application Publication 2004/0123141 (hereinafter '141) in further view of Moran U.S. Patent No. 7,085,936 (hereinafter '936).

As to independent claim 14, "A system for protecting an electronic network, comprising: a plurality of agents with the electronic network, the agents being grouped into at least one cooperative agent cell having one cell delegate" is taught in '239 col. 5, lines 12-37;

"a communications protocol within each cooperative agent cell, for (a) communicating between agents of the cooperative agent cell, and (b) communicating with cell delegates external to the cooperative agent cell" is shown in '239 col. 3, lines 4-10 and col. 22, lines 27-31;

the following is not explicitly taught in '239:

"means for determining normal activity levels of the electronic network" however '358 teaches determining normal behavior in col. 3, lines 6-26;

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system of a cooperative response to threat to domain security taught in '239 to include a mechanism to perform an initial assessment. One of ordinary skill in the art would have been motivated to perform such a modification to improve the efficiency of protection required by the increasingly sophisticated attacks see '358 (col. 1, lines 19 et seq.)

following is not explicitly taught in '239 and '358:

"means for detecting malicious activity" however '141 teaches the agents block the abnormal activity by shutting down an application in paragraph 52.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a method or system of a cooperative response to threat to domain security taught in '239 and '358 to include a mechanism to stop an attack. One of ordinary skill in the art would have been motivated to perform such a modification because of the many inadequacies in current detection systems see '141 (paragraph 5).

following is not explicitly taught in '239, '141 and '358:

"means for counter-intelligence to reveal the origin of the malicious activity" however '936 teaches in col. 33, lines 34-40 the use of a database information to trace the origins of files;

"means for isolating compromised components of the electronic network" however '936 teaches that the system includes a trap system create a virtual cage in col. 7, lines 42-51;

"means for repairing damage caused by the malicious activity; means for determining vulnerabilities in the current protection provided by the plurality of agents;

and means for improving protection to resist future attack on the electronic network" however '936 teaches "The inventive system focuses on discovering and presenting information about an attack, and presents configuration problems that are likely related to the attack, while suppressing those that aren't. Additionally, the presentation may show where relevant configuration problems fit within the factors that made the attack possible. This facilitates recovering from the attack, because the system administrator may be able to block future attacks of the same type by fixing only a subset of factors involved rather than having to fix every possible factor. It is also extremely useful in situations where one of the configuration problems cannot be changed due to its providing crucial functionality for the enterprise. For example, the restore command should normally not be set to allow execution by normal users with SetUID to root because it can be used to allow a normal user to install his own SetUID program on the computer that gives him a root shell. However, the dump-restore command pair have features that make them preferable in various circumstances to the other commonly available archiving and file copying utilities, and thus a system administrator may decide that having this capability available is worth the security risk" in col. 12, lines 9-29.

Conclusion

8. It is noted, PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN "The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA

1968)). A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments (see MPEP 2123).

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/ELLEN TRAN/
Primary Examiner, Art Unit 2433
24 April 2009